

UNCLASSIFIED



# **NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY**



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

## **NDSLIC DISCLAIMER**

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

## **QUICK LINKS**

[North Dakota](#)

[Emergency Services](#)

[Regional](#)

[Energy](#)

[National](#)

[Food and Agriculture](#)

[International](#)

[Government Sector \(including  
Schools and Universities\)](#)

[Banking and Finance Industry](#)

[Information Technology and  
Telecommunications](#)

[Chemical and Hazardous Materials  
Sector](#)

[Public Health](#)

[Commercial Facilities](#)

[Transportation](#)

[Communications Sector](#)

[Water and Dams](#)

[Critical Manufacturing](#)

[North Dakota Homeland Security  
Contacts](#)

[Defense Industrial Base Sector](#)

UNCLASSIFIED

## UNCLASSIFIED

### **NORTH DAKOTA**

**(North Dakota) 2,000 barrels of water spill in North Dakota.** The North Dakota Department of Health reported September 3 that a leak in the Denbury Onshore-owned Paynter Source Well in Bismarck caused 2,000 barrels of water used for enhanced oil recovery to spill in Bowman County September 1.

[http://www.wahpetondailynews.com/article\\_1f28165e-342f-11e4-b436-001a4bcf887a.html](http://www.wahpetondailynews.com/article_1f28165e-342f-11e4-b436-001a4bcf887a.html)

**(North Dakota) No one hurt when train derails at Dickinson.** Crews were able to quickly contain a natural gas leak that resulted from a crash when four flatbed railcars and boxcars derailed from a BNSF train in Dickinson September 6.

<http://www.jamestownsun.com/content/no-one-hurt-when-train-derails-dickinson>

**(North Dakota) Woman dies of West Nile in North Dakota.** The first West Nile virus-related death in North Dakota for 2014 was reported Tuesday. A woman, older than 60, died after being hospitalized. She had no previous health conditions, North Dakota Department of Health West Nile Virus Surveillance Coordinator Alicia Lepp said. [http://bismarcktribune.com/news/state-and-regional/woman-dies-of-west-nile-in-north-dakota/article\\_12f93ad8-386d-11e4-b5f1-0019bb2963f4.html](http://bismarcktribune.com/news/state-and-regional/woman-dies-of-west-nile-in-north-dakota/article_12f93ad8-386d-11e4-b5f1-0019bb2963f4.html)

**(Fargo) West Acres Shopping Center in lockdown after assault report.** Police were still looking Thursday night for the man who reportedly assaulted a West Acres mall employee earlier in the day, sending the mall into a brief lockdown. Police got the call about 11 a.m. that an armed man attacked a woman near the J.C. Penney store, said department spokesman Lt. Joel Vettel.

<http://www.inforum.com/content/suspect-sought-assault-led-lockdown-west-acres-mall>

### **REGIONAL**

**(Minnesota) Computer glitch may have exposed student data.** The Minnesota Office of Higher Education announced September 5 that a coding error on the State's Student Educational Loan Fund program may have compromised the

## UNCLASSIFIED

## UNCLASSIFIED

private information, including Social Security numbers, of college students seeking loans after it was discovered the weekend of August 30. Officials are investigating and will notify all students affected by the glitch.

<http://www.startribune.com/local/274181251.html?page=all&prepage=1&c=y>

### **NATIONAL**

**(National)** **With Islamic State speech, Obama deepens US involvement in Middle East.** President Obama strove to differentiate this new battle with terrorists 'unique in their brutality' from the wars he inherited, in particular the war in Iraq. His intervention rationale placed a priority on humanitarian reasons.

<http://www.csmonitor.com/USA/Foreign-Policy/2014/0911/With-Islamic-State-speech-Obama-deepens-US-involvement-in-Middle-East-video>

**(National)** **Virus hitting Midwest could be 'tip of iceberg,' CDC official says.** The U.S. Centers for Disease Control and Prevention's Division of Viral Diseases is investigating a recent bout of Enterovirus EV-D68, a respiratory virus that has sent about 475 children to hospitals in at least 10 States.

<http://www.cnn.com/2014/09/07/health/respiratory-virus-midwest/index.html>

**(National)** **Audit: Homeland Security 'ill-prepared' for potential pandemics.** The DHS inspector general released a report September 8 that found that the department's preparations for pandemic events were inadequate due to lack of proper inventory controls, supply-replenishment plans, and adherence to department guidelines. DHS management agreed with the inspector general's recommendations, with some issues previously identified and acted upon.

<http://www.washingtonpost.com/blogs/federal-eye/wp/2014/09/08/audit-homeland-security-ill-prepared-for-potential-pandemics/>

### **INTERNATIONAL**

**(International)** **Home Depot confirms months-long hack.** Home Depot representatives confirmed September 8 that the company's payment systems were breached as early as April 2014 and the attack went unnoticed until September 2 when banking institutions reported unusual activity connected to debit and credit card data from the company's stores in the U.S. and Canada. The company is working with the U.S. Secret Service to determine the scope of the

## UNCLASSIFIED

## UNCLASSIFIED

breach and has implemented additional security measures at its stores.

<http://money.cnn.com/2014/09/08/technology/security/home-depot-breach/index.html>

**(International) Hackers break into Healthcare.gov.** The U.S. Department of Health and Human Services announced September 4 that hackers were able to successfully install malicious software on Healthcare.gov that could have been used to launch an attack on other sites from the federal insurance portal in July. The intrusion was detected August 25 and mitigated after technicians determined that no consumer data was taken.

<http://abcnews.go.com/Health/wireStory/hackers-break-healthcare-25252518>

**(International) Chinese attack groups operate in parallel in cyber espionage campaigns: FireEye.** Researchers with FireEye discovered two cyberespionage campaigns originating in two regions of China that appear to share several commonalities including using the same custom backdoors and remote access trojans (RATs). One campaign dubbed Moafee targets various military, government, and defense industry entities while the second known as DragonOK targets high-tech and manufacturing companies in Taiwan and Japan.

<http://www.securityweek.com/chinese-attack-groups-operate-parallel-cyber-espionage-campaigns-fireeye>

## **BANKING AND FINANCE INDUSTRY**

**(International) Cybercriminals love PayPal, financial phishing on the rise.**

Kaspersky Lab researchers released statistics on spam and phishing emails for the month of July, which found that phishing emails targeting financial services increased 7.9 percent during the month, with PayPal being the most targeted company. The researchers also found that the overall share of spam in all email traffic increased 2.2 percent to a total of 67 percent during July, among other findings. <http://www.net-security.org/secworld.php?id=17320>

**(International) Six corporate executives and six corporate entities indicted for orchestrating a \$500 million offshore asset protection, securities fraud, and money laundering scheme.** Six individuals from the U.S., Canada, Belize, and the Bahamas and six corporate entities were indicted September 9 for allegedly operating an elaborate scheme to enable U.S. citizens to circumvent and evade

## UNCLASSIFIED

## UNCLASSIFIED

securities and tax laws by setting up fake companies to evade taxes and engage in money laundering. The alleged scheme laundered around \$500 million between 2009 and 2014. <http://www.fbi.gov/newyork/press-releases/2014/six-corporate-executives-and-six-corporate-entities-indicted-for-orchestrating-a-500-million-offshore-asset-protection-securities-fraud-and-money-laundering-scheme>

### **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

Nothing Significant to Report

### **COMMERCIAL FACILITIES**

**(Iowa) Bomb detonated at Waterloo park.** Police responded to the Riverview Recreational Area in Waterloo August 30 and detonated a homemade explosive device made of sections of pipe and nails that was found by a volunteer cleaning the park. Authorities are investigating the incident.

[http://wcfcourier.com/news/local/crime-and-courts/bomb-detonated-at-waterloo-park/article\\_416a476d-0179-5607-9049-c0ced0c0189b.html](http://wcfcourier.com/news/local/crime-and-courts/bomb-detonated-at-waterloo-park/article_416a476d-0179-5607-9049-c0ced0c0189b.html)

### **COMMUNICATIONS SECTOR**

Nothing Significant to Report

### **CRITICAL MANUFACTURING**

**(International) Rigged industrial software site points to watering hole attack.**

Researchers at AlienVault reported that the Web site of an unnamed industrial software company was compromised with a piece of reconnaissance malware called Scanbox that collected information on visitors to the site, including visitors' IP addresses, language, operating system, and security programs. The unnamed company produces system engineering and simulation software for several industries including manufacturing, automotive, and aerospace firms.

<http://www.computerworld.com/article/2600767/security/rigged-industrial-software-site-points-to-watering-hole-attack.html>

**(International) Kidde recalls smoke and combination smoke/CO alarms due to alarm failure.** Kidde announced a recall for around 1.3 million Kidde hard-wired

UNCLASSIFIED

## UNCLASSIFIED

smoke and combination smoke/carbon monoxide (CO) alarms in the U.S. and Canada due to the potential for the alarms to fail to alert consumers of fire or CO hazards following a power outage. <http://www.cpsc.gov/en/Recalls/2014/Kidde-Recalls-Smoke-and-Combination-SmokeCO-Alarms/>

### **DEFENSE/ INDUSTRY BASE SECTOR**

**(National)** Pratt & Whitney halted F135 deliveries over titanium sourcing issues. Officials at Pratt & Whitney, a division of United Technologies, stated that the company suspended deliveries of its F-135 engines for the F-35 Lightning II Joint Strike Fighter for a 3-week period during May due to a pedigree validation issue with a titanium supplier. More than 100 aircraft were retrofitted with a replacement fan variable arm to address the issue. <http://www.janes.com/article/42664/pratt-whitney-halted-f135-deliveries-over-titanium-sourcing-issues>

### **EMERGENCY SERVICES**

**(Tennessee)** 30 teens escape from Nashville detention center. Officers continued to search for the remaining seven teenagers September 2 who were part of a group of 30 juveniles that escaped from the Woodland Hills Youth Development Center in Nashville September 1 through a weak spot in a fence. <http://news.msn.com/crime-justice/30-teens-escape-from-nashville-detention-center>

**(New York)** NY detective accused of leaking secret documents. A Suffolk County police detective pleaded guilty September 9 to one charge of official misconduct for stealing confidential law enforcement documents, including police tour and intelligence reports, active criminal investigation information, and personnel information, and leaking them to a newspaper. <http://www.newsday.com/news/region-state/da-ny-detective-stole-leaked-confidential-papers-1.9271536>

### **ENERGY**

**(National)** Enterprise proposes crude oil pipeline from North Dakota to Oklahoma. Enterprise Products Partners L.P. hopes to succeed where many

UNCLASSIFIED



## UNCLASSIFIED

others have failed to build a new pipeline to carry oil from North Dakota's booming Bakken oil fields to the nation's central oil storage facility in Cushing, Oklahoma.

[http://www.bizjournals.com/denver/blog/earth\\_to\\_power/2014/09/enterprise-proposes-crude-oil-pipeline-from-north.html](http://www.bizjournals.com/denver/blog/earth_to_power/2014/09/enterprise-proposes-crude-oil-pipeline-from-north.html)

### **FOOD AND AGRICULTURE**

**(Minnesota)** Cabbage likely caused Minnesota E. coli outbreak. Minnesota Department of Health officials reported August 29 that green whole head cabbage was likely the source of an E. coli outbreak that sickened 15 individuals in July. Officials believe the cabbage was contaminated before the out-of-State supplier distributed it to at least 10 restaurants across Minnesota.

<http://kimt.com/2014/08/30/cabbage-likely-caused-minnesota-e-coli-outbreak/>

**(Colorado)** Massive fire destroys fertilizer plant in sterling. Ten workers safely shut off liquid fertilizer chemical tanks and evacuated the Kugler Company fertilizer plant in Sterling September 3 after a welding accident sparked a fire that consumed nearly 95 percent of the building. A reverse 9-1-1 call was transmitted to 200 households warning residents that a small amount of anhydrous ammonia leaked out of pipes during the blaze and could pose health risks to individuals with respiratory problems. <http://denver.cbslocal.com/2014/09/03/massive-fire-destroys-fertilizer-plant-in-sterling/>

### **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

**(Louisiana)** Louisiana experiences second data breach with state-issued debit cards. JP Morgan Chase notified Louisiana's government that the company's security system was breached and hackers may have accessed the personal information of residents using prepaid debit cards issued by 3 State agencies.

[http://www.nola.com/politics/index.ssf/2014/08/louisiana\\_experiences\\_second\\_d.html](http://www.nola.com/politics/index.ssf/2014/08/louisiana_experiences_second_d.html)

**(Wisconsin)** Crisis team available to Pulaski students after crash. One person was killed and seven others were injured, including six students, after a car crashed into the back of a Pulaski School District bus on Highway 29 westbound and Saint

UNCLASSIFIED



## UNCLASSIFIED

Augustine Road in Wisconsin September 2 closing westbound lanes of the highway for about 5 hours.

<http://www.wbay.com/story/26432366/2014/09/02/crash-involving-school-bus-closes-hwy-29>

**(California) Hacker may have sent bomb threat at O.C. schools; no explosives found.** Fountain Valley High School and Valley Vista High in California were both evacuated and classes were cancelled September 3 after school administrators received an emailed threat of a potential attack. Police continue to investigate and found no explosive devices on campus, after determining that a student's account was hacked prompting the threatening email.

<http://www.latimes.com/local/lanow/la-me-ln-fountain-valley-high-bomb-threat-20140903-story.html>

**(California) \$200,000 financial aid scam hits Bay Area College.** College of Marin authorities in California are investigating an alleged financial aid scam believed to involve 23 individuals posing as students to fraudulently obtain \$200,000 in federal financial aid. The suspects allegedly enrolled in online classes with the university, then withdrew from school soon after financial aid was distributed.

<http://www.sfgate.com/crime/article/200-000-plot-to-steal-financial-aid-hits-Bay-5749273.php>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**(International) FBI starts investigation of celeb photo hack.** The FBI stated that it began an investigation to identify and apprehend the individuals behind a leak of personal photos belonging to several celebrities that were stored in Apple's iCloud service. <http://news.softpedia.com/news/FBI-Starts-Investigation-of-Celeb-Photo-Hack-457278.shtml>

**(International) Syrian Malware Team makes use of enhanced BlackWorm RAT.** FireEye researchers reported that a hacktivist group known as the Syrian Malware Team has used an enhanced version of the BlackWorm remote access trojan (RAT) known as "Dark Edition" in its campaigns. The new variant allows attackers to bypass user account control (UAC) features, spread itself over network drives, and disable firewalls. <http://www.scmagazine.com/syrian-malware-team-makes-use-of-enhanced-blackworm-rat/article/368902/>

## UNCLASSIFIED

**(International) Linux systems infiltrated and controlled in a DDoS botnet.**

Researchers at Akamai Technologies reported that Linux systems could be at risk of infections using Iptables and Iptablex to compromise systems and use them in distributed denial of service (DDoS) attacks. The researchers reported that the infections appeared to be caused by a large number of Linux-based Web servers being compromised via Apache Struts, Tomcat, and Elasticsearch vulnerabilities.

<http://www.net-security.org/secworld.php?id=17322>

**(International) CERT warns of Android apps vulnerable to MitM attacks.** The Computer Emergency Response Team Coordination Center at Carnegie Mellon University (CERT/CC) published a list of popular Android apps that expose users to man-in-the-middle (MitM) attacks due to the apps not properly validating SSL certificates. CERT/CC released its findings in a spreadsheet detailing their results and is attempting to contact the authors of every app that failed the organization's tests. <http://www.securityweek.com/cert-warns-android-apps-vulnerable-mitm-attacks>

**(International) Home router DNS settings changed via Web-based attack.**

Kaspersky Lab researchers identified a Web-based attack that uses Web pages with malicious scripts to attempt to change users' home router Domain Name System (DNS) settings in order to redirect users to phishing pages of financial institutions. The attack was mostly observed in Brazil but also targeted some users in the U.S., Canada, Mexico, and other countries.

<http://news.softpedia.com/news/Home-Router-DNS-Settings-Changed-Via-Web-Based-Attack-457668.shtml>

**(International) Cyberespionage group starts using new Mac OS X backdoor program.** FireEye researchers found that a cyberespionage group dubbed GREF has recently begun using a backdoor program known as XSLCmd that targets Mac OS X systems in order to steal files and install additional malware. The GREF group is known for attacks on several sectors including the U.S. defense industry as well as electronics manufacturers, engineering firms, and non-governmental organizations worldwide.

<http://www.networkworld.com/article/2603441/cyberespionage-group-starts-using-new-mac-os-x-backdoor-program.html>

## UNCLASSIFIED

### **PUBLIC HEALTH**

**(National) Unidentified Respiratory Virus Likely to Hit Kids Across Country.** A respiratory illness that has already sickened more than a thousand children in 10 states is likely to become a nationwide problem, doctors say. The disease hasn't been officially identified but officials suspect a rare respiratory virus called human enterovirus 68. <http://abcnews.go.com/Health/unidentified-respiratory-virus-hit-kids-country/story?id=25334106>

### **TRANSPORTATION**

**(Florida) Third flight diverted, woman removed over seat dispute.** A Delta flight from New York headed towards West Palm Beach diverted to Jacksonville September 2 after a passenger became combative and demanded the airplane land after an altercation with another passenger and flight attendants. [http://seattletimes.com/html/nationworld/2024441533\\_apxplanedivertedseatrecliner.html](http://seattletimes.com/html/nationworld/2024441533_apxplanedivertedseatrecliner.html)

**(Washington) Person detained after security incident on plane at Sea-Tac Airport.** A Southwest Airlines flight from Seattle to Denver was delayed for 4 hours September 11 after a potential threat was discovered when a passenger on board the plane used threatening names for his Wi-Fi hot spot such as "Southwest – Bomb On Board" and "Bomb Location 19E." All passengers aboard the plane were rescreened and later reboarded the plane while the man responsible for the threat was detained by authorities. <http://www.kirotv.com/news/news/person-detained-after-incident-plane-sea-tac-airpo/nhLMj/>

### **WATER AND DAMS**

**(Minnesota) Boil water order continues in Brainerd.** A boil water advisory remained in effect for residents in Brainerd following a water main break and storm that knocked out power to Brainerd's municipal water pumps. Officials stated that they may lift the advisory as soon as September 9 if water tests are satisfactory. <http://www.kare11.com/story/news/local/2014/09/08/boil-water-order-continues-in-brainerd/15317439/>

## UNCLASSIFIED

UNCLASSIFIED

## **NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295(IN ND ONLY); Email: [ndslic@nd.gov](mailto:ndslic@nd.gov); Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of Criminal Investigation (BCI):** 701-328-5500; **North Dakota Highway Patrol:** 701-328-2455; **US Attorney's Office Intel Analyst:** 701-297-7400; **Bismarck FBI:** 701-223-4875; **Fargo FBI:** 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security [dthanson@nd.gov](mailto:dthanson@nd.gov), 701-328-8165

UNCLASSIFIED